

# National Cyber Alert System

[Archive](#)

## Cyber Security Bulletin SB09-306

### Vulnerability Summary for the Week of October 26, 2009

The US-CERT Cyber Security Bulletin provides a summary of new vulnerabilities that have been recorded by the National Institute of Standards and Technology (NIST) National Vulnerability Database (NVD) in the past week. The NVD is sponsored by the Department of Homeland Security (DHS) National Cyber Security Division (NCSD) / United States Computer Emergency Readiness Team (US-CERT). For modified or updated entries, please visit the [NVD](#), which contains historical vulnerability information.

The vulnerabilities are based on the [CVE](#) vulnerability naming standard and are organized according to severity, determined by the [Common Vulnerability Scoring System](#) (CVSS) standard. The division of high, medium, and low severities correspond to the following scores:

- **High** - Vulnerabilities will be labeled High severity if they have a CVSS base score of 7.0 - 10.0
- **Medium** - Vulnerabilities will be labeled Medium severity if they have a CVSS base score of 4.0 - 6.9
- **Low** - Vulnerabilities will be labeled Low severity if they have a CVSS base score of 0.0 - 3.9

Entries may include additional information provided by organizations and efforts sponsored by US-CERT. This information may include identifying information, values, definitions, and related links. Patch information is provided when available. Please note that some of the information in the bulletins is compiled from external, open source reports and is not a direct result of US-CERT analysis.

High Vulnerabilities				
Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
acoustica -- mp3_audio_mixer	Heap-based buffer overflow in Acoustica MP3 Audio Mixer 2.471 allows remote attackers to cause a denial of service (crash) or execute arbitrary code via a long string in a .M3U playlist file.	2009-10-27	9.3	<a href="#">CVE-2009-3810</a> XF VUPEN MILWORM SECUNIA OSVDB
adam_gerson -- moodle_counselist	SQL injection vulnerability in Moodle Course List 6.x before 6.x-1.2, a module for Drupal, allows remote attackers to execute arbitrary SQL commands via unspecified vectors.	2009-10-26	7.5	<a href="#">CVE-2009-3778</a> VUPEN BID CONFIRM
assistanttools -- music_tag_editor	Stack-based buffer overflow in Music Tag Editor 1.61 build 212 allows remote attackers to execute arbitrary code via an MP3 file with a long ID3 tag. NOTE: some of these details are obtained from third party information.	2009-10-27	9.3	<a href="#">CVE-2009-3811</a> XF MILWORM SECUNIA OSVDB MISC
cutepdf -- formmax	Heap-based buffer overflow in FormMax (formerly AcroForm) evaluation 3.5 allows remote attackers to cause a denial of service or possibly execute arbitrary code via a crafted FormMax import (.aim) file. NOTE: the provenance	2009-10-26	9.3	<a href="#">CVE-2009-3790</a> XF SECUNIA

	of this information is unknown; the details are obtained solely from third party information.			<a href="#">SECUNIA OSVDB</a>
dedecms -- dedecms	SQL injection vulnerability in feedback_js.php in DedeCMS 5.1 allows remote attackers to execute arbitrary SQL commands via the arcurl parameter.	2009-10-27	<a href="#">7.5</a>	<a href="#">CVE-2009-3806</a> <a href="#">BUGTRAQ</a>
fijiwebdesign -- com_ajaxchat	PHP remote file inclusion vulnerability in Fiji Web Design Ajax Chat (com_ajaxchat) component 1.0 for Joomla! allows remote attackers to execute arbitrary PHP code via a URL in the GLOBALS[mosConfig_absolute_path] parameter to tests/ajcuser.php.	2009-10-28	<a href="#">7.5</a>	<a href="#">CVE-2009-3822</a> <a href="#">VUPEN</a> <a href="#">BID</a> <a href="#">MISC</a> <a href="#">SECUNIA</a>
flagbit -- fb_filebase	SQL injection vulnerability in the Flagbit Filebase (fb_filebase) extension 0.1.0 for TYPO3 allows remote attackers to execute arbitrary SQL commands via unspecified vectors.	2009-10-28	<a href="#">7.5</a>	<a href="#">CVE-2009-3820</a> <a href="#">CONFIRM</a>
kramware -- mixsense_dj_studio	MixSense DJ Studio 1.0.0.1 allows remote attackers to cause a denial of service (application crash) and possibly execute arbitrary code via a long string in an .mp3 playlist file.	2009-10-27	<a href="#">9.3</a>	<a href="#">CVE-2009-3808</a> <a href="#">XF</a> <a href="#">MILWoRM</a>
linux -- kernel linux -- kernel	Integer overflow in the kvm_dev_ioctl_get_supported_cpuid function in arch/x86/kvm/x86.c in the KVM subsystem in the Linux kernel before 2.6.31.4 allows local users to have an unspecified impact via a KVM_GET_SUPPORTED_CPUID request to the kvm_arch_dev_ioctl function.	2009-10-29	<a href="#">7.2</a>	<a href="#">CVE-2009-3638</a> <a href="#">CONFIRM</a> <a href="#">XF</a> <a href="#">BID</a> <a href="#">CONFIRM</a> <a href="#">CONFIRM</a> <a href="#">MLIST</a> <a href="#">MLIST</a> <a href="#">CONFIRM</a>
michael_j_greenwood -- php_content_manager	Directory traversal vulnerability in include/processor.php in Greenwood PHP Content Manager 0.3.2 allows remote attackers to include and execute arbitrary local files via a ..(dot dot) in the content_path parameter.	2009-10-28	<a href="#">7.5</a>	<a href="#">CVE-2009-3824</a> <a href="#">XF</a> <a href="#">MILWoRM</a>
mixvibes -- mixvibes	Stack-based buffer overflow in MixVibes 7.043 Pro allows remote attackers to cause a denial of service (crash) via a long string in a .vib file.	2009-10-27	<a href="#">9.3</a>	<a href="#">CVE-2009-3807</a> <a href="#">XF</a> <a href="#">MILWoRM</a>
mozilla -- firefox	Array index error in Mozilla Firefox 3.0.x before 3.0.15 and 3.5.x before 3.5.4 allows remote attackers to execute arbitrary code via a long string that triggers incorrect memory allocation and a heap-based buffer overflow during conversion to a floating-point number.	2009-10-29	<a href="#">10.0</a>	<a href="#">CVE-2009-1563</a> <a href="#">CONFIRM</a>
mozilla -- firefox	Use-after-free vulnerability in Mozilla Firefox 3.5.x before 3.5.4 allows remote attackers to cause a denial of service (application crash) or possibly execute arbitrary code by creating JavaScript web-workers recursively.	2009-10-29	<a href="#">10.0</a>	<a href="#">CVE-2009-3371</a> <a href="#">CONFIRM</a>
mozilla -- firefox mozilla -- seamonkey	Mozilla Firefox before 3.0.15 and 3.5.x before 3.5.4, and SeaMonkey before 2.0, allows remote attackers to execute arbitrary code via a crafted regular expression in a Proxy Auto-configuration (PAC) file.	2009-10-29	<a href="#">9.3</a>	<a href="#">CVE-2009-3372</a> <a href="#">CONFIRM</a>
mozilla -- firefox mozilla -- seamonkey	Heap-based buffer overflow in the GIF image parser in Mozilla Firefox before 3.0.15 and 3.5.x before 3.5.4, and SeaMonkey before 2.0, allows remote attackers to execute arbitrary code via unspecified vectors.	2009-10-29	<a href="#">10.0</a>	<a href="#">CVE-2009-3373</a> <a href="#">CONFIRM</a>
	The XPCVariant::VariantDataToJS function in the XPCOM implementation in Mozilla Firefox 3.0.x before 3.0.15 and			

mozilla -- firefox	3.5.x before 3.5.4 does not enforce intended restrictions on interaction between chrome privileged code and objects obtained from remote web sites, which allows remote attackers to execute arbitrary JavaScript with chrome privileges via unspecified method calls, related to "doubly-wrapped objects."	2009-10-29	7.5	CVE-2009-3374 CONFIRM
mozilla -- firefox mozilla -- seamonkey	Mozilla Firefox before 3.0.15 and 3.5.x before 3.5.4, and SeaMonkey before 2.0, does not properly handle a right-to-left override (aka RLO or U+202E) Unicode character in a download filename, which allows remote attackers to spoof file extensions via a crafted filename, as demonstrated by displaying a non-executable extension for an executable file.	2009-10-29	9.3	CVE-2009-3376 CONFIRM CONFIRM
mozilla -- firefox	Multiple unspecified vulnerabilities in liboggz before cf5feeaab69b05e24, as used in Mozilla Firefox 3.5.x before 3.5.4, allow remote attackers to cause a denial of service (application crash) or possibly execute arbitrary code via unknown vectors.	2009-10-29	10.0	CVE-2009-3377 CONFIRM CONFIRM
mozilla -- firefox	The oggplay_data_handle_theora_frame function in media/liboggplay/src/liboggplay/oggplay_data.c in liboggplay, as used in Mozilla Firefox 3.5.x before 3.5.4, attempts to reuse an earlier frame data structure upon encountering a decoding error for the first frame, which allows remote attackers to cause a denial of service (NULL pointer dereference and application crash) or possibly execute arbitrary code via a crafted .ogg video file.	2009-10-29	9.3	CVE-2009-3378 CONFIRM
mozilla -- firefox	Multiple unspecified vulnerabilities in libvorbis, as used in Mozilla Firefox 3.5.x before 3.5.4, allow remote attackers to cause a denial of service (application crash) or possibly execute arbitrary code via unknown vectors. NOTE: this might overlap CVE-2009-2663.	2009-10-29	10.0	CVE-2009-3379 CONFIRM CONFIRM
mozilla -- firefox	Multiple unspecified vulnerabilities in the browser engine in Mozilla Firefox 3.0.x before 3.0.15 and 3.5.x before 3.5.4 allow remote attackers to cause a denial of service (memory corruption and application crash) or possibly execute arbitrary code via unknown vectors.	2009-10-29	10.0	CVE-2009-3380 CONFIRM
mozilla -- firefox	Multiple unspecified vulnerabilities in the browser engine in Mozilla Firefox 3.5.x before 3.5.4 allow remote attackers to cause a denial of service (memory corruption and application crash) or possibly execute arbitrary code via unknown vectors.	2009-10-29	10.0	CVE-2009-3381 CONFIRM
mozilla -- firefox	layout/base/nsCSSFrameConstructor.cpp in the browser engine in Mozilla Firefox 3.0.x before 3.0.15 does not properly handle first-letter frames, which allows remote attackers to cause a denial of service (memory corruption and application crash) or possibly execute arbitrary code via unspecified vectors.	2009-10-29	10.0	CVE-2009-3382 CONFIRM
mozilla -- firefox	Multiple unspecified vulnerabilities in the JavaScript engine in Mozilla Firefox 3.5.x before 3.5.4 allow remote attackers to cause a denial of service (memory corruption and application crash) or possibly execute arbitrary code via unknown vectors.	2009-10-29	10.0	CVE-2009-3383 CONFIRM CONFIRM CONFIRM
opendocman -- opendocman	SQL injection vulnerability in index.php in OpenDocMan 1.2.5 allows remote attackers to execute arbitrary SQL commands via the frmuser (aka Username) parameter.	2009-10-26	7.5	CVE-2009-3788 BID
opendocman	SQL injection vulnerability in index.php in OpenDocMan 1.2.5 allows remote attackers to execute arbitrary SQL			CVE-2009-

openocman -- opendocman	commands via the frmpass (aka Password) parameter. NOTE: the provenance of this information is unknown; the details are obtained solely from third party information.	2009-10-27	<a href="#">7.5</a>	<a href="#">3801 SECUNIA</a>
ordasoft -- com_booklibrary	PHP remote file inclusion vulnerability in doc/releasenote.php in the BookLibrary (com_booklibrary) component 1.0 for Joomla! allows remote attackers to execute arbitrary PHP code via a URL in the mosConfig_absolute_path parameter, a different vector than CVE-2009-2637. NOTE: the provenance of this information is unknown; the details are obtained solely from third party information.	2009-10-28	<a href="#">7.5</a>	<a href="#">CVE-2009-3817 VUPEN MISC BID</a>
otslabs -- otsav_dj otslabs -- otsav_radio otslabs -- otsav_tv	Heap-based buffer overflow in OtsAV DJ trial version 1.85.64.0, Radio trial version 1.85.64.0, TV trial version 1.85.64.0, and Free version 1.77.001 allows remote attackers to execute arbitrary code via a long playlist in an Ots File List (.ofl) file.	2009-10-27	<a href="#">9.3</a>	<a href="#">CVE-2009-3812 XF VUPEN MILWORM SECUNIA MISC OSVDB</a>
qemu -- qemu	Multiple use-after-free vulnerabilities in vnc.c in the VNC server in QEMU 0.10.6 and earlier might allow guest OS users to execute arbitrary code on the host OS by establishing a connection from a VNC client and then (1) disconnecting during data transfer, (2) sending a message using incorrect integer data types, or (3) using the Fuzzy Screen Mode protocol, related to double free vulnerabilities.	2009-10-23	<a href="#">8.5</a>	<a href="#">CVE-2009-3616 CONFIRM CONFIRM CONFIRM MLIST MLIST CONFIRM MLIST CONFIRM CONFIRM</a>
quicksketch -- filefield	The filefield_file_download function in FileField 6.x-3.1, a module for Drupal, does not properly check node-access permissions for Drupal core private files, which allows remote attackers to access unauthorized files via unspecified vectors.	2009-10-26	<a href="#">7.5</a>	<a href="#">CVE-2009-3781 BID CONFIRM CONFIRM CONFIRM CONFIRM</a>
sahana -- sahana	Directory traversal vulnerability in www/index.php in Sahana 0.6.2.2 allows remote attackers to include and execute arbitrary local files via a .. (dot dot) in the mod parameter.	2009-10-26	<a href="#">7.5</a>	<a href="#">CVE-2009-3625 CONFIRM MLIST MLIST CONFIRM</a>
stanislas_rollback -- sr_freecap	Unspecified vulnerability in the session handling feature in freeCap CAPTCHA (sr_freecap) extension 1.2.0 and earlier for TYPO3 has unknown impact and attack vectors.	2009-10-28	<a href="#">10.0</a>	<a href="#">CVE-2009-3818 CONFIRM</a>
thomas_graber -- gencms	Multiple directory traversal vulnerabilities in GenCMS 2006 allow remote attackers to include and execute arbitrary local files via a .. (dot dot) in the (1) p parameter to show.php and the (2) Template parameter to admin/pages/SiteNew.php.	2009-10-28	<a href="#">7.5</a>	<a href="#">CVE-2009-3825 XF MILWORM</a>
urs_maag -- maag_randomimage	Unspecified vulnerability in the Random Images (maag_randomimage) extension 1.6.4 and earlier for TYPO3 allows remote attackers to execute arbitrary shell commands via unspecified vectors.	2009-10-28	<a href="#">10.0</a>	<a href="#">CVE-2009-3819 CONFIRM</a>

[Back to top](#)

Medium Vulnerabilities					
Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info	
ac4p -- mobilelib_gold	Directory traversal vulnerability in myhtml.php in Mobilelib GOLD 3.0, when magic_quotes_gpc is enabled, allows remote attackers to read arbitrary files via a .. (dot dot) in the GLOBALS[page] parameter.	2009-10-28	5.0	CVE-2009-3823 XF MILWoRM	
acoustica -- mp3_audio_mixer	Acoustica MP3 Audio Mixer 1.0 and possibly 2.471 allows remote attackers to cause a denial of service (crash) via a long string in a .sgp playlist file.	2009-10-27	4.3	CVE-2009-3809 XF VUPEN MILWoRM	
amirocms -- amiro.cms	Amiro.CMS 5.4.0.0 and earlier allows remote attackers to obtain sensitive information via an invalid loginname ("%%") to _admin/index.php, which reveals the installation path and other information in an error message.	2009-10-27	5.0	CVE-2009-3802 XF VUPEN MISC SECUNIA MISC	
amirocms -- amiro.cms	Multiple cross-site scripting (XSS) vulnerabilities in Amiro.CMS 5.4.0.0 and earlier allow remote attackers to inject arbitrary web script or HTML via the status_message parameter to (1) /news, (2) /comment, (3) /forum, (4) /blog, and (5) /tags; the status_message parameter to (6) forum.php, (7) discussion.php, (8) guestbook.php, (9) blog.php, (10) news.php, (11) srv_updates.php, (12) srv_backups.php, (13) srv_twist_prevention.php, (14) srv_tags.php, (15) srv_tags_reindex.php, (16) google_sitemap.php, (17) sitemap_history.php, (18) srv_options.php, (19) locales.php and (20) plugins_wizard.php in _admin/; a crafted IMG BBcode tag in the message body of a (21) forum, (22) guestbook, or (23) comment; (24) the content of an avatar file, which is not properly handled by Internet Explorer; and (25) the loginname parameter (aka username) in _admin/index.php.	2009-10-27	4.3	CVE-2009-3803 XF XF VUPEN MISC SECUNIA MISC	
apache -- solr	Cross-site scripting (XSS) vulnerability in the Apache Solr Search (solr) extension 1.0.0 for TYPO3 allows remote attackers to inject arbitrary web script or HTML via unspecified vectors.	2009-10-28	4.3	CVE-2009-3821 CONFIRM	
ashok_modi -- abuse	Cross-site scripting (XSS) vulnerability in Abuse 5.x before 5.x-2.1 and 6.x before 6.x-1.1-alpha1, a module for Drupal, allows remote attackers to inject arbitrary web script or HTML via unspecified vectors.	2009-10-26	4.3	CVE-2009-3780 BID CONFIRM CONFIRM CONFIRM	
derrick_oswald -- html-parser	The decode_entities function in util.c in HTML-Parser before 3.63 allows context-dependent attackers to cause a denial of service (infinite loop) via an incomplete SGML numeric character reference, which triggers generation of an invalid UTF-8 character.	2009-10-29	4.3	CVE-2009-3627 CONFIRM VUPEN BID MLIST	
gpg4win -- gpg4win	gpg2.exe in Gpg4win 2.0.1, as used in KDE Kleopatra 2.0.11, allows remote attackers to cause a denial of service (application crash) via a long certificate signature.	2009-10-27	4.3	CVE-2009-3805 XF BID MISC	

ibm -- lotus_connections	Multiple cross-site scripting (XSS) vulnerabilities in Activities pages in the Mobile subsystem in IBM Lotus Connections 2.5.0.0 allow remote attackers to inject arbitrary web script or HTML via unspecified vectors.	2009-10-28	4.3	CVE-2009-3816 CONFIRM
moshe_weitzman -- og_vocab	Cross-site scripting (XSS) vulnerability in Organic Groups (OG) Vocabulary 5.x before 5.x-1.1, a module for Drupal, allows remote attackers to inject arbitrary web script or HTML via the group title.	2009-10-26	4.3	CVE-2009-3786 VUPEN BID CONFIRM CONFIRM
mozilla -- firefox	Mozilla Firefox before 3.0.15, and 3.5.x before 3.5.4, allows remote attackers to read form history by forging mouse and keyboard events that leverage the auto-fill feature to populate form fields, in an attacker-readable form, with history entries.	2009-10-29	5.0	CVE-2009-3370 CONFIRM
mozilla -- firefox	content/html/document/src/nsHTMLDocument.cpp in Mozilla Firefox 3.0.x before 3.0.15 and 3.5.x before 3.5.4 allows user-assisted remote attackers to bypass the Same Origin Policy and read an arbitrary content selection via the document.getSelection function.	2009-10-29	4.3	CVE-2009-3375 CONFIRM
mutt -- mutt	mutt_ssl.c in mutt 1.5.19 and 1.5.20, when OpenSSL is used, does not properly handle a '\o' character in a domain name in the subject's Common Name (CN) field of an X.509 certificate, which allows man-in-the-middle attackers to spoof arbitrary SSL servers via a crafted certificate issued by a legitimate Certification Authority, a related issue to CVE-2009-2408.	2009-10-23	6.8	CVE-2009-3765 MLIST MLIST SUSE CONFIRM
mutt -- mutt	mutt_ssl.c in mutt 1.5.16, when OpenSSL is used, does not verify the domain name in the subject's Common Name (CN) field of an X.509 certificate, which allows man-in-the-middle attackers to spoof SSL servers via an arbitrary valid certificate.	2009-10-23	6.8	CVE-2009-3766 CONFIRM
novell -- opensuse novell -- suse_linux	iscsi_discovery in open-iscsi in SUSE openSUSE 10.3 through 11.1 and SUSE Linux Enterprise (SLE) 10 SP2 and 11 allows local users to overwrite arbitrary files via a symlink attack on an unspecified temporary file that has a predictable name.	2009-10-23	4.4	CVE-2009-1297 SUSE
opendocman -- opendocman	Multiple cross-site scripting (XSS) vulnerabilities in OpenDocMan 1.2.5 allow remote attackers to inject arbitrary web script or HTML via the last_message parameter to (1) add.php, (2) toBePublished.php, (3) index.php, and (4) admin.php; the PATH_INFO to the default URI to (5) category.php, (6) department.php, (7) profile.php, (8) rejects.php, (9) search.php, (10) toBePublished.php, (11) user.php, and (12) view_file.php; and (13) the caller parameter in a Modify User action to user.php.	2009-10-26	4.3	CVE-2009-3789 BID
openldap -- openldap	libraries/libldap/tls_o.c in OpenLDAP, when OpenSSL is used, does not properly handle a '\o' character in a domain name in the subject's Common Name (CN) field of an X.509 certificate, which allows man-in-the-middle attackers to spoof arbitrary SSL servers via a crafted certificate issued by a legitimate Certification Authority, a related issue to CVE-2009-2408.	2009-10-23	6.8	CVE-2009-3767 VUPEN CONFIRM MLIST MLIST SUSE
perl -- perl	Perl 5.10.1 allows context-dependent attackers to cause a denial of service (application crash) via a UTF-8 character with a large, invalid codepoint, which is not properly handled during a regular-expression match.	2009-10-29	5.0	CVE-2009-3626 VUPEN CONFIRM

proftpd -- proftpd	The mod_tls module in ProFTPD before 1.3.2b, and 1.3.3 before 1.3.3rc2, when the dNSNameRequired TLS option is enabled, does not properly handle a '\o' character in a domain name in the Subject Alternative Name field of an X.509 client certificate, which allows remote attackers to bypass intended client-hostname restrictions via a crafted certificate issued by a legitimate Certification Authority, a related issue to CVE-2009-2408.	2009-10-28	5.8	CVE-2009-3639 CONFIRM BID
runcms -- runcms	Multiple SQL injection vulnerabilities in modules/forum/post.php in RunCMS 2M1 allow remote authenticated users to execute arbitrary SQL commands via (1) the pid parameter, which is not properly handled by the store function in modules/forum/class/class.forumposts.php, or (2) the topic_id parameter.	2009-10-27	6.5	CVE-2009-3804 SECUNIA MISC
runcms -- runcms	Multiple SQL injection vulnerabilities in RunCMS 2M1 allow remote authenticated users to execute arbitrary SQL commands via the (1) forum parameter to modules/forum/post.php and possibly (2) forum_id variable to modules/forum/class/class.permissions.php.	2009-10-27	6.5	CVE-2009-3813 SECUNIA MISC
runcms -- runcms	Static code injection vulnerability in RunCMS 2M1 allows remote authenticated administrators to execute arbitrary PHP code via the "Filter/Banning" feature, as demonstrated by modifying modules/system/cache/bademails.php using the "Prohibited: Emails" action, and other unspecified filters.	2009-10-27	6.5	CVE-2009-3814 MISC
runcms -- runcms	RunCMS 2M1, when running with certain error_reporting levels, allows remote attackers to obtain sensitive information via (1) the op[] parameter to modules/contact/index.php or (2) uid[] parameter to userinfo.php, which leaks the installation path in an error message when these parameters are used in a call to the preg_match function.	2009-10-27	5.0	CVE-2009-3815 MISC
sjoerd_arendsen -- simplenews_statistics	Cross-site scripting (XSS) vulnerability in Simplenews Statistics 6.x before 6.x-2.0, a module for Drupal, allows remote attackers to inject arbitrary web script or HTML via unspecified vector.	2009-10-26	4.3	CVE-2009-3783 BID CONFIRM CONFIRM
sjoerd_arendsen -- simplenews_statistics	Open redirect vulnerability in Simplenews Statistics 6.x before 6.x-2.0, a module for Drupal, allows remote attackers to redirect users to arbitrary web sites and conduct phishing attacks via unspecified vectors.	2009-10-26	6.8	CVE-2009-3784 BID CONFIRM CONFIRM
sjoerd_arendsen -- simplenews_statistics	Multiple cross-site request forgery (CSRF) vulnerabilities in Simplenews Statistics 6.x before 6.x-2.0, a module for Drupal, allow remote attackers to hijack the authentication of arbitrary users via unknown vectors.	2009-10-26	6.8	CVE-2009-3785 BID CONFIRM CONFIRM
snort -- snort	Snort before 2.8.5.1, when the -v option is enabled, allows remote attackers to cause a denial of service (application crash) via a crafted IPv6 packet that uses the (1) TCP or (2) ICMP protocol.	2009-10-28	4.3	CVE-2009-3641 BID CONFIRM FULLDISC
squidguard -- squidguard	Buffer overflow in sgLog.c in squidGuard 1.3 and 1.4 allows remote attackers to cause a denial of service (application hang or loss of blocking functionality) via a long URL with	2009-10-28	5.0	CVE-2009-3700 VUPEN CONFIRM

	many / (slash) characters, related to "emergency mode."			<a href="#">CONFIRM</a> <a href="#">BID</a>
squidguard -- squidguard	Multiple buffer overflows in squidGuard 1.4 allow remote attackers to bypass intended URL blocking via a long URL, related to (1) the relationship between a certain buffer size in squidGuard and a certain buffer size in Squid and (2) a redirect URL that contains information about the originally requested URL.	2009-10-28	<a href="#">5.0</a>	<a href="#">CVE-2009-3826</a> <a href="#">VUPEN</a> <a href="#">BID</a>
stefan_auditor -- vcard	Cross-site scripting (XSS) vulnerability in vCard 5.x before 5.x-1.4 and 6.x before 6.x-1.3, a module for Drupal, allows remote attackers to inject arbitrary web script or HTML via unspecified vectors, related to the addition of the theme_vcard function to a theme and the use of default content.	2009-10-26	<a href="#">4.3</a>	<a href="#">CVE-2009-3779</a> <a href="#">VUPEN</a> <a href="#">CONFIRM</a> <a href="#">CONFIRM</a> <a href="#">CONFIRM</a>
vivvo -- vivvo	files.php in Vivvo CMS 4.1.5.1 allows remote attackers to conduct directory traversal attacks and read arbitrary files via the file parameter with "logs/" in between two . (dot) characters, which is filtered into a "../" sequence.	2009-10-26	<a href="#">5.0</a>	<a href="#">CVE-2009-3787</a> <a href="#">MISC</a> <a href="#">BID</a> <a href="#">BUGTRAQ</a> <a href="#">SECUNIA</a>

[Back to top](#)

### Low Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
2bits -- userpoints	Unspecified vulnerability in Userpoints 6.x before 6.x-1.1, a module for Drupal, allows remote authenticated users with "View own userpoints" permissions to read the userpoint data of arbitrary users via unknown attack vectors.	2009-10-26	<a href="#">3.5</a>	<a href="#">CVE-2009-3782</a> <a href="#">VUPEN</a> <a href="#">BID</a> <a href="#">CONFIRM</a> <a href="#">CONFIRM</a>
linux -- kernel linux -- kernel	The update_cr8_intercept function in arch/x86/kvm/x86.c in the KVM subsystem in the Linux kernel before 2.6.32-rc1 does not properly handle the absence of an Advanced Programmable Interrupt Controller (APIC), which allows local users to cause a denial of service (NULL pointer dereference and system crash) or possibly gain privileges via a call to the kvm_vepu_ioctl function.	2009-10-29	<a href="#">2.1</a>	<a href="#">CVE-2009-3640</a> <a href="#">XF</a> <a href="#">BID</a> <a href="#">CONFIRM</a> <a href="#">MLIST</a> <a href="#">MLIST</a> <a href="#">CONFIRM</a>

[Back to top](#)**Last updated November 02, 2009**
 Print This Document